**Yee &
Associates, P.C.**

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Brandon S. Hoffman** **Group Art Unit 2136**	Facsimile No.: **571/273-8300**
From: Stephanie Fay Legal Assistant to Hope Shimabuku	No. of Pages Including Cover Sheet: **32**

Message:

Enclosed herewith:

- Transmittal Document; and
- Appeal Brief.

Re: Application No. **09/687,100**
Attorney Docket No: **AUS9-2000-0401-US1**

Date: Monday, March 06, 2006

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	*This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.*

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Gusler et al.**	§	Group Art Unit: **2136**
	§	
Serial No.: **09/687,100**	§	Examiner: **Hoffman, Brandon S.**
	§	
Filed: **October 12, 2000**	§	Attorney Docket No.: **AUS9-2000-0401-US1**
	§	
For: **Method and System for Building Dynamic Firewall Rules, Based on Content of Downloaded Documents**		

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

<u>Certificate of Transmission Under 37 C.F.R. § 1.8(a)</u>
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on March 6, 2006.

By: Stephanie Fay
Stephanie Fay

TRANSMITTAL OF APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37)

No fee is believed to be necessary. If, however, a fee is required, please charge this fee to IBM Corporation Deposit Account No. 09-0447. In the event that any additional fees are required for the prosecution of this application, please charge any necessary fees to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is needed, the extension is requested and the fee for this extension should be charged to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Hope Shimabuku

Hope Shimabuku
Registration No. 57,072
Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEYS FOR APPLICANTS

Docket No. AUS9-2000-0401-US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Gusler et al.** §
§ Group Art Unit: **2136**
Serial No. **09/687,100** §
§ Examiner: **Hoffman, Brandon S.**
Filed: **October 12, 2000** §
§
For: **Method and System for Building Dynamic Firewall Rules, Based on Content of Downloaded Documents** §
§

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

<u>Certificate of Transmission Under 37 C.F.R. § 1.8(a)</u>
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on March 6, 2006.

By: Stephanie Fay
Stephanie Fay

<u>APPEAL BRIEF (37 C.F.R. 41.37)</u>

This brief is in furtherance of the Notice of Appeal, filed in this case on February 1, 2006.

No fee is believed to be necessary. If, however, a fee is required, please charge this fee to IBM Corporation Deposit Account No. 09-0447. In the event that any additional fees are required for the prosecution of this application, please charge any necessary fees to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is needed, the extension is requested and the fee for this extension should be charged to IBM Corporation Deposit Account No. 09-0447.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation, as reflected in the Assignment recorded on October 12, 2000, at Reel 011279, Frame 0659.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-15

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 2 and 9
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1, 3-8, and 10-15
4. Claims allowed: None
5. Claims rejected: 1, 3-8, and 10-15
6. Claims objected to: None

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 3-8, and 10-15

STATUS OF AMENDMENTS

All of the amendments to the claims have been entered. No amendments have been filed in this case subsequent to the final rejection dated November 25, 2005.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

Claim 1 recites a method for filtering incoming data from an external computer network. (Specification page 4, lines 4-6). A firewall is coupled to the external computer network, and a server computer system is coupled to an internal computer network. A plurality of clients is coupled to the server computer system and is unable to access the external computer network directly. (Specification page 6, lines 4-12; Figure 1). The firewall receives a document from the external computer network. (Specification page 7, lines 24-27). The firewall then determines whether the document is from a known blocked site. (Specification page 7, lines 27-32). In response to determining that the document is from a known blocked site, the firewall blocks the document without scanning the document. (Specification page 7, line 32 through page 8, lines 2). The firewall then determines whether the document is from a known safe site. (Specification page 8, lines 3-9). In response to determining that the document is from a known safe site, the firewall forwards the document to the server without scanning the document. (Specification page 8, lines 9-12). All of the plurality of clients are permitted to access the forwarded document. (Specification page 6, lines 4-12; specification page 8, lines 9-12; specification page 9, lines 17-19; Figure 1). In response to determining that the document is not from a known blocked site or a known safe site, the firewall scans text fields included in the document for pre-selected keyword(s). (Specification page 4, lines 6-9; specification page 8, lines 13-24). The firewall blocks the document if any of the text fields include content that contains pre-selected keywords. (Specification page 4, lines 9-11; specification page 8, lines 25-26). The server computer system is prohibited from receiving the document in response to the document being blocked. (Specification page 6, lines 4-12; specification page 7, line 31 through page 8, line 1; specification page 8, lines 25 through page 9, line 5; Figure 1). The firewall indicates that a site that sent the document is a known blocked site by adding the address of the site to a filtering table. (Specification page 4, lines 9-14; specification page 8, line 25 through page 9, line 5).

B. CLAIM 5 – DEPENDENT

Claim 5 further describes the method of claim 1, specifically adding to the step of indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of a site to a filtering table. The step further includes adding the address of the site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords. (Specification page 4, lines 9-14; specification page 8, lines 25 through page 9, line 5).

C. CLAIM 6 – DEPENDENT

Claim 6 further describes the method of claim 1. The method implements the addition of a site to the filtering table using a strong text parsing language. (Specification page 8, lines 13-24).

D. CLAIM 7 – DEPENDENT

Claim 7 further describes the method of claim 1, wherein the instance of the filter is periodically refreshed to enact the updated filtering table. (Specification page 9, lines 6-16).

E. CLAIM 8 – INDEPENDENT

Claim 8 describes a computer program product in a computer readable medium for use in a data processing system for filtering incoming data from an external computer network. (Specification page 4, lines 4-6). The computer program product includes a firewall coupled to the external computer network. A server computer system is coupled to an internal computer network. A plurality of clients is coupled to the server computer system and is unable to access the external computer network directly. (Specification page 6, lines 4-12; Figure 1). The computer program product also includes instructions for receiving at the firewall a document from the external computer network. (Specification page 7, lines 24-27). The computer program product has instructions for determining, by the firewall, whether the document is from a known blocked site. (Specification page 7, lines 27-32). In response to determining that the document is from a known blocked site, the computer program product includes instructions for blocking the document without scanning the document. (Specification page 7, line 32 through page 8, lines 2). The computer program product also has instructions for determining, by the firewall, whether the document is from a known safe site. (Specification page 8, lines 3-9). In response to determining that the document is from a known safe site, the computer program product also has instructions for forwarding the document to the server without scanning the document. (Specification page 8, lines 9-12). All of the plurality of clients are permitted to access the forwarded document. (Specification page 6, lines 4-12; specification page 8, lines 9-12; specification page 9, lines 17-19; Figure 1). In response to determining that the document is not from a known blocked site or a known safe site, the computer program product includes instructions for scanning, by the firewall, text fields included in the document for pre-selected keyword(s). (Specification page 8, lines 12-23). The computer program product also has instructions for blocking, by the firewall, the document if any of the text fields include content that contains pre-selected keywords. (Specification page 4, lines 6-9; specification page 8, lines 13-24). The server computer system is prohibited from receiving the document in response to the document being blocked. (Specification page 6, lines 4-12; specification page 7, line 31 through page 8, line 1; specification page 8, lines 25 through page 9, line 5; Figure 1). The computer program product has instructions for indicating that a site that sent the document is a known blocked site by adding, by the firewall, the address of the site to a filtering table. (Specification page 4, lines 9-14; specification page 8, line 25 through page 9, line 5).

F. CLAIM 12 – DEPENDENT

Claim 12 further describes the computer program product of claim 8, specifically adding to the instructions for indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of a site to a filtering table. The instructions further includes instructions for adding the address of the site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords. (Specification page 4, lines 9-14; specification page 8, lines 25 through page 9, line 5).

G. CLAIM 13 – DEPENDENT

Claim 13 further describes the computer program product of claim 8. The computer program product implements the instructions for addition of a site to the filtering table using a strong text parsing language. (Specification page 8, lines 13-24).

H. CLAIM 14 – DEPENDENT

Claim 14 further describes the computer program product of claim 8, wherein the instance of the filter is periodically refreshed to enact the updated filtering table. (Specification page 9, lines 6-16).

I. CLAIM 15 - INDEPENDENT

Claim 15 recites a system for filtering incoming data from an external computer network. (Specification page 4, lines 4-6). The system includes a firewall coupled to the external computer network. The system also includes a server computer system coupled to an internal computer network. The system includes a plurality of clients coupled to the server computer system, wherein the plurality of clients is unable to access the external computer network directly. (Specification page 6, lines 4-12; Figure 1). The system has a firewall that receives a document from the external computer network. (Specification page 7, lines 24-27). The system has the firewall determine whether the document is from a known blocked site. (Specification page 7, lines 27-32). In response to determining that the document is from a known blocked site, the system has the firewall block the document without scanning the document. (Specification page 7, line 32 through page 8, lines 2). The system then has the firewall determine whether the document is from a known safe site. (Specification page 8, lines 3-9). In response to determining that the document is from a known safe site, the system has the firewall forward the document to the server without scanning the document. (Specification page 8, lines 9-12). All of the plurality of clients are permitted to access the forwarded document. (Specification page 6, lines 4-12; specification page 8, lines 9-12; specification page 9, lines 17-19; Figure 1). In response to determining that the document is not from a known blocked site or a known safe site, the system has the firewall scan text fields included in the document for pre-selected keyword(s). (Specification page 4, lines 6-9; specification page 8, lines 13-24). The system then has the firewall block the document if any of the text fields include content that contains pre-selected keywords. (Specification page 4, lines 9-11; specification page 8, lines 25-26). The system includes a server computer system that is prohibited from receiving the document in response to the document being blocked. (Specification page 6, lines 4-12; specification page 7, line 31 through page 8, line 1; specification page 8, lines 25 through page 9, line 5; Figure 1). The system then has the firewall indicate that a site that sent the document is a known blocked site by adding the address of the site to a filtering table. (Specification page 4, lines 9-14; specification page 8, line 25 through page 9, line 5).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1, 3-8 and 10-15)

Claims 1, 3-8 and 10-15 stand rejected under 35 U.S.C. § 102(e) as anticipated over *Massarani*, Content-Indexing Search System and Method Providing Search Results Consistent with Content Filtering and Blocking Policies Implemented in a Blocking Engine, U.S. Patent No. 6,336,117 (January 1, 2002) (hereinafter "*Massarani*").

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1, 3-8 and 10-15)

A.1. CLAIMS 1, 3-4, 8, 10-11, AND 15 UNDER 35 U.SC. § 102(e)

The examiner rejects claims 1, 3-4, 10-11, and 15 under 35 U.S.C. § 102(e) as anticipated by *Massarani*, Content-Indexing Search System and Method Providing Search Results Consistent with Content Filtering and Blocking Policies Implemented in a Blocking Engine, U.S. Patent No. 6,336,117 (January 1, 2002) (hereinafter "*Massarani*"). This rejection is respectfully traversed.

The examiner states that:

> Regarding claims 1, 8, and 15, Massarani teaches a method/system/computer program product in a computer readable medium for use in a data processing system for filtering incoming data from an external computer network, the method/system/computer program product comprising:
>
> - A firewall that is coupled to said external computer network (fig. 1, ref. num 126/127/135/136);
> - A server computer system coupled to an internal computer network (fig. 1, ref. num 124);
> - A plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly (fig. 1, ref. num 102/104);
> - Receiving, at said firewall, a document from said external computer network (fig. 3, ref. num 308 and col. 6, lines 14-16);
> - Determining, by said firewall, whether said document is from a known blocked site (fig. 3, ref. num 312 and col. 6, lines 20-22);
> - In response to determining that said document is from a known blocked site, blocking, by said firewall, said document without scanning said document (fig. 3, ref. num 312 and col. 6, lines 20-22);
> - Determining, by said firewall, whether said document is from a know safe site (fig. 3, ref. num 310 and col. 6, lines 17-19);
> - In response to determining that said document is from a known safe site, forwarding, by said firewall, said document without scanning said document, all of said plurality of clients being permitted to access said forwarded document (fig. 3, ref. num 312 and col. 6, lines 20-22);
> - In response to determining that said document is not from a known blocked site or a know safe site, scanning, by said firewall, text fields included in said document for pre-selected keywords (fig. 3, ref. num 316 and col. 6, lines 27-29);

- Blocking, by said firewall, the document if any of said text fields include content that contains pre-selected keywords (fig. 3, ref. num 316 and col. 6, lines 27-29);
- Said server computer system being prohibited from receiving said document in response to said document being blocked (fig. 3, ref. num 316 and col. 6, lines 27-29); and
- Indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table (col. 6, lines 27-29 and col. 7, lines 25-30).

Office Action dated November 25, 2005, pages 3-4.

Regarding claim 1, *Massarani* does not anticipate claim 1 because *Massarani* fails to show all the limitations of claim 1. A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994).

Claim 1 is the representative claim in this group of claims. Claim 1 is as follows:

> 1. A method for filtering incoming data from an external computer network, comprising:
>
> a firewall that is coupled to said external computer network;
>
> a server computer system coupled to an internal computer network;
>
> a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;
>
> receiving, at said firewall, a document from said external computer network;
>
> determining, by said firewall, whether said document is from a known blocked site;
>
> in response to determining that said document is from a known blocked site, blocking, by said firewall, said document without scanning said document;
>
> determining, by said firewall, whether said document is from a known safe site;
>
> in response to determining that said document is from a known safe site, forwarding, by said firewall, said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;
>
> in response to determining that said document is not from a known blocked site or a known safe site, scanning, by said firewall, text fields included in said document for pre-selected keyword(s);

> blocking, by said firewall, the document if any of said text fields include content that contains pre-selected keywords;
>
> said server computer system being prohibited from receiving said document in response to said document being blocked; and
>
> indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table.

Massarani does not anticipate claim 1 because *Massarani* does not show the feature of indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table. The examiner asserts that *Massarani* does show the feature, but the examiner misapprehends the cited sections of this reference.

First, the examiner asserts that *Massarani* does show the feature of adding, by said firewall, the address of said site to a filtering table by referring specifically to column 6, lines 27-29 and column 7, lines 30-32 of *Massarani*. In an examiner interview held on September 27, 2005, the examiner additionally referred to column 7, lines 21-24. The cited sections are as follows:

> [Column 6, lines 27-29] In step 316, if an exclusionary keyword list is specified, the document text is scanned and the document is excluded if it contains one or more keywords in the list.
>
> [Column 7, lines 21-24] In step 507, any document found in the cache is added to the indexing database as complying with the blocking filtering policy to one or more user groups in local installation.
>
> [Column 7, lines 25-30] The primary advantage of the process of FIG. 5 is the application of the filtering and blocking rules is done only once by the engine designed to do so, i.e., the caching and blocking engine. The scanning and indexing operation is performed on a local (high performance) copy of the target content, rather than the more variable Internet content sites.

Massarani, column 6, lines 27-29 and column 7, lines 21-30.

The cited sections of *Massarani* describe the process of blocking a document requested by the user in an internet search request if the document contains certain keywords. The cited sections also detail the process of searching and filtering internal source sites, i.e. an intranet, rather than external websites. The internal search process includes adding any document within the repository of internal source sites into an indexing database. An indexing database is a database tree defined by a certain user group with specific content filtering rules as described in column 6, lines 8-13 of *Massarani*. Column 6, lines 8-13 are as follows:

> In step 306, multiple indexing database trees are created as needed and each tree is associated with a user group as defined in the content filtering rules. For example, one indexing database tree for children with a strict PICs filtering rule; one tree for adults with more liberal filtering rules.

Massarani, column 6, lines 8-13.

Column 7, lines 25-30 of the cited text describes the asserted primary advantage of the *Massarani* process, that filtering and blocking rules are done only once rather than multiple times. However, none of the cited texts describe adding an address of a site to a filtering table that sent a document from a known blocked site.

On the other hand, the claimed invention does add, by a firewall, an internet address of a site to the filtering table if a document is sent from a site not currently listed in the known blocked site list. Claim 1 specifically recites that an indication is made that the site is a known blocked site by adding the address of the site to the filtering table. In contrast, *Massarani* only adds allowed documents to the indexing database but not the addresses of the sites that sent rejected documents.

Moreover, the fact that the filtering and blocking rules are only done once as stated in *Massarani* does not necessarily lead to the conclusion that the reason that the process is only done once is because the internet address is added to the filtering table. *Massarani* never states such a conclusion and the inference that such a conclusion exists impermissibly broadens the scope of *Massarani*. Furthermore, the examiner admits in the Office Action, and Appellants agree, that *Massarani* does not show the feature of adding an address of a known blocked site to a filtering table. In the Office Action, the examiner states (emphasis added):

> Massarani does not explicitly say that blocked sites are added to the list (Massarani explicitly says blocked sites are blocked, but doesn't mention if they are added to the list).

Office Action dated November 25, 2005, page 6.

Thus, by the examiner's own admission, *Massarani* does not show all the features of the presently claimed invention.

Moreover, the "spirit and scope" statement in *Massarani* and used by the examiner in the response to Applicant's last Response to Office Action does not address the feature of adding blocked site addresses to a filtering table. In the Office Action, the examiner states:

> [H]owever, column 8, lines 4-6, say that various changes can be made therein without departing from the spirit and scope of the invention. Adding blocked sites for the same reason as adding allowed sites would be an obvious change that wouldn't depart from the spirit and scope of the invention. The idea is that a site that is a good site should remain good; the same applied for bad sites. For example, PBS.com is cached locally and determined to be a good site. PBS.com does not need to be scanned again because PBS.com will not become a bad site. On the other hand, a site that contains inappropriate content is cached locally and determined to be a bad site. The bad site does not need to be scanned again because the bad site will not become a good site.

Office Action dated November 25, 2005, page 6.

The test of whether a reference anticipates the features of the claimed invention is whether each and every element of the claimed invention is identically shown in that single reference. *See In re Bond*, 910 F.2d at 832, 15 U.S.P.Q.2d at 1567. Whether a change is obvious in an invention does not meet the test criterion for an anticipation rejection. As a matter of fact, a reference that must be changed proves that the reference does not identically show all the elements of the claimed invention. Thus, in the present case, a change to *Massarani* to add a known blocked site by adding an address to a filtering table demonstrates that *Massarani* does not meet the test criterion for an anticipation rejection and proves that all the elements of the claimed invention are not present in *Massarani*. Furthermore, nowhere does the cited reference teach that indicating that a site that sent the document is a known blocked site by adding the address of the site to a filtering table as recited in the indicating step of claim 1. Since *Massarani* neither teaches nor identically shows the feature, *Massarani* does not anticipate claim 1.

Additionally, the "spirit and scope" statement is too broad to conclude that adding blocked sites is disclosed in that statement. The cited text from *Massarani* is as follows:

> Various changes can be made therein without departing from the spirit and scope of the invention as defined in the appended claims.

Massarani, column 8, lines 4-6.

A change that does not "depart from the spirit and scope of the invention" is a very broad statement that does not specifically point to any feature in particular. Therefore, *Massarani* does not disclose all of the features of the present invention explicitly. Moreover, the features of the present invention do not necessarily follow based on the statement cited by the examiner. If the examiner wishes to propose that *Massarani* could be changed, that is an obviousness rejection that cannot be made in the context of a rejection under 35 U.S.C. § 102.

Furthermore, the PBS.com example used by the examiner still does not address the feature of adding blocked site addresses to a filtering table. Appellants assume that the examiner uses the PBS.com as an example of what would be included in the "spirit and scope" statement. However, *Massarani* does not disclose this example anywhere in the reference. Additionally, as indicated above, the "spirit and scope" statement is so broad that, without something more specific in *Massarani* itself, the examiner cannot assume that the "spirit and scope" statement includes such an example. Furthermore, even if *Massarani* does intend to include the PBS.com example in the "spirit and scope" statement, the PBS.com example still does not disclose the feature of adding a blocked site to a filtering table. The examiner states in the Office Action that a bad site will be "cached locally and determined to be a bad site" and that the bad site "does not need to be scanned again because the bad site will not become a good site." *Office Action* dated November 25, 2005, page 6. However, the actions of caching, determining, and scanning of a bad site still do not show the feature of adding a blocked site to a filtering table.

Moreover, *Massarani* also does not inherently anticipate the feature of adding, by a firewall, an internet address to the filtering table if a document is sent from a site not currently listed in the known blocked site list. To inherently anticipate, the features of the present invention must be necessarily present and not just be a possible feature or step. Although not specifically stated in the Office Action, Applicants interpret the examiner's comment regarding the "spirit and scope of the invention" to refer to the concept of inherent anticipation. However, if referring to the concept, the examiner has misapplied the concept of inherent anticipation, because the "spirit and scope" statement is too broad to meet requirements of inherent anticipation.

Section 102 of Title 35 deals with novelty and loss of patent rights. An invention is said to be "anticipated" when it is squarely described or disclosed in a single reference as identified from one of the categories of 35 U.S.C. § 102, commonly referred to as "prior art". Express anticipation occurs when the invention is expressly disclosed in the prior art, patent or publication. In some cases, however, when the claimed invention is not described *in haec verba*, the "doctrine of inherency" is relied on to establish anticipation. Under the principles of inherency, a claim is anticipated if a structure in the prior art necessarily functions in accordance with the limitations of a process or method claim. *In re King*, 801 F.2d 1324, 231 U.S.P.Q. 136 (Fed. Cir. 1986). A prior art reference that discloses all of a patent's claim limitations anticipates that claim even though the reference does not expressly disclose the "inventive concept" or desirable property the patentee discovered. *Verdgaal Brothers, Inc. v. Union Oil Company of California*, 814 F.2d 628, 2 U.S.P.Q.2d 1051, (Fed. Cir. 1987). Mere possibilities or even probabilities, however, are not enough to establish inherency. The missing claimed characteristics must be a "natural result" flowing from what is disclosed. *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 20 U.S.P.Q.2d 1746 (Fed. Cir. 1991). Unstated elements in a reference are inherent when they exist as a "matter of scientific fact". *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 7 U.S.P.Q.2d 1057 (Fed. Cir.), *cert. denied*, 488 U.S. 892 (1988) and *Hughes Aircraft Co. v. United States*, 8 U.S.P.Q.2d 1580 (Ct. Cl. 1988). Otherwise, the invention is not inherently anticipated.

The feature of adding a blocked site to a filtering table is not a necessarily present element that is naturally resulting or existing as a matter of scientific fact from *Massarani*. As stated above, the feature of adding a blocked site to a filtering table is only a mere possibility of what was meant to be disclosed in the "spirit and scope" statement. Thus, the mere possibility of the feature is not enough to establish inherency. Additionally, a document and an internet address are not elements that naturally result from each other. A document and an internet address are two different objects altogether. A document is a writing that provides information. An internet address is a unique identifier to facilitate communication across the internet. The existence of a document does not naturally result in the existence of an internet address and vice versa. Additionally, the existence of a document does not necessitate the need for an internet address and vice-versa. Thus, the fact that a document is added to an indexing database does not naturally result in a blocked internet protocol address being added to a filtering table. Thus, the feature is not necessarily present and is not inherently anticipated by *Massarani*. Since *Massarani* does not inherently or expressly show the feature of indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table, *Massarani* does not anticipate claim 1.

Because claims 8 and 15 cover the same subject matter as claim 1, the same distinctions between claim 1 and *Massarani* apply to claims 8 and 15. Because claims 3-4 and 10-11 depend from claims 1 and 8, the same distinctions between *Massarani* and the claimed invention in claims 1 and 8 also apply for these claims. Therefore, the rejection of claims 1, 3-8, 10-11, and 15 under 35 U.S.C. § 102(e) has been overcome.

A.2. Claims 5 and 12

The examiner has rejected claims 5 and 12 under 35 U.S.C. § 102(e) as anticipated by *Massarani*. This rejection is respectfully traversed.

Regarding claims 5 and 12, the examiner states that:

> Regarding claims 5 and 12, Massarani teaches wherein the step of indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of a site to a filtering table further comprises adding the address of the site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords (col. 6, lines 27-29 and col. 7, lines 25-30).

Office Action dated November 25, 2005, page 5.

Claim 5 is representative in this group of claims. *Massarani* does not anticipate claim 5 because *Massarani* fails to show all the limitations of claim 5. Claim 5 provides as follows:

> 5. The method according to claim 1, wherein the step of indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of a site to a filtering table further comprises adding the address of the site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords.

Massarani does not show the feature of adding the address of the site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords. The feature of claim 5 is an additional step within the indicating step of claim 1. As indicated above, *Massarani* does not show the feature of indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of a site to a filtering table from claim 1. Therefore, *Massarani* also does not show the additional step within the indicating step of claim 1. Accordingly, *Massarani* does not anticipate claim 5.

Additionally, since claim 5 depends from claim 1, all the arguments presented above for claim 1 also apply to claim 5. Also, because claim 12 covers the same subject matter as claim 5, the same distinctions between claim 5 and *Massarani* apply to claim 12. Therefore, the rejection of claims 5 and 12 under 35 U.S.C. § 102(e) has been overcome.

A.3. Claims 6 and 13

The examiner has rejected claims 6 and 13 under 35 U.S.C. § 102(e) as anticipated by *Massarani*. This rejection is respectfully traversed.

Regarding claims 6 and 13, the examiner states that:

> Regarding claims 6 and 13, Massarani teaches wherein the instructions for addition of a site to the filtering table are implemented in a strong text parsing language (col. 5, lines 32-39).

Office Action dated November 25, 2005, page 5.

Regarding claim 6, *Massarani* does not anticipate claim 6 because *Massarani* fails to show all the limitations of claim 6. Claim 6 is representative of this group of claims. Claim 6 is as follows:

> 6. The method according to claim 1, wherein the addition of a site to the filtering table is implemented using a strong text parsing language.

Massarani does not show the feature of the addition of a site to the filtering table is implemented using a strong text parsing language. The examiner asserts that *Massarani* does show the claimed feature by referring specifically to column 5, lines 32-39. However, the examiner misapprehends the cited text. The cited text is as follows:

> [Column 5, lines 32-39] More specifically, PICS Rules is a language for expressing filtering rules (profiles) that allow or block access to URLs based on PICS labels that describe those URLs. The labels are created using a software tool in accordance with a PICS Technical specification-1.1 available in the Internet at http://www.w#.org/PICS/. The software tool is used to create labels in a document that describe particular URLs. Alternatively, in lieu of pasting the labels into documents, an independent reader distributes the labels through a separate server called a Label Bureau. Filtering software will know to check at that Label Bureau to find the labels much as a consumer knows to read particular magazines for review of appliances or automobiles. Once the label has been created, the label is inserted as an extra header in the HTTP header stream that precedes the content of the documents that are sent to the web browser.

Massarani, column 5, lines 32-39.

The cited text describes the use of PICS Rules to facilitate the filtering rules that allow or block access to URLs. The cited text indicates that PICS Rules use a form of labels to describe a particular URL. The labels are used to help apply the filtering rules in *Massarani*. However, the cited text does not describe using a strong text parsing language to add a site to the filtering table. The cited text describes using PICS rules to allow and block access but does not disclose using the PICS rules to add a site to a filtering table as in the present invention.

Additionally, PICS as described in *Massarani* is not the same as a strong text parsing language. According to the cited text, PICS is a language for expressing filtering rules. *See Massarani*, column 5, line 33. On the other hand, a strong text parsing language is a method for scanning and reading the content of an HTML document. A method for reading is not the same thing as a language for expressing filtering rules. Therefore, *Massarani* does not disclose the feature of adding a site to a filtering table using a strong text parsing language.

Moreover, as shown above, *Massarani* does not anticipate all the features of claim 1. Since claim 6 depends from claim 1, then all arguments for claim 1 also apply here and *Massarani* does not anticipate all the features of claim 6.

Because claim 13 covers the same subject matter as claim 6, the same distinctions between claim 6 and *Massarani* apply to claim 13. Therefore, the rejection of claims 6 and 13 under 35 U.S.C. § 102(e) has been overcome.

A.4. Claims 7 and 14

The examiner has rejected claims 7 and 14 under 35 U.S.C. § 102(e) as anticipated by *Massarani*. This rejection is respectfully traversed.

Regarding claims 7 and 14, the examiner states that:

> Regarding claims 7 and 14, Massarani teaches wherein the instance of the filter is periodically refreshed to enact the updated filtering tables (col. 6, lines 33-40).

Office Action dated November 25, 2005, page 5.

Regarding claim 7, *Massarani* does not anticipate claim 7 because *Massarani* fails to show all the limitations of claim 7. Claim 7 is representative of this group of claims. Claim 7 provides as follows:

> 7. The method according to claim 1, wherein the instance of the filter is periodically refreshed to enact the updated filtering tables.

Massarani does not show the feature of an instance of the filter is periodically refreshed to enact the updated filtering table. The examiner asserts that *Massarani* does show the claimed feature by referring specifically to column 6, lines 33-40. However, the examiner misapprehends the cited text. The cited text is as follows:

> [Column 6, lines 33-40] The advantage of the process of FIG. 3 is that all additional (exclusion) processing is performed in the database indexing phase. There is little additional processing needed on the users search processing and presentation phases. Presumably, search operations are much more frequent than indexing operations in the life cycle of a search engine, even with re-scanning of content for possible changes.

Massarani, column 6, lines 33-40.

The cited text describes the advantage of performing additional processes in the database indexing phase. *Massarani* indicates that the processing time is reduced because additional processing is small in the search processing and presentation phases. However, the cited text does not disclose that a filter is periodically refreshed to enact an updated filtering table. The cited text refers to the rescanning of content for possible changes, but the rescanning of content is not the same as periodically refreshing the filter. Additionally, the rescanning of content is not the same thing as updating a filtering table. *Massarani* does not state anywhere in the reference that the act of rescanning refers to refreshing a filter or updating a filtering table. Thus, *Massarani* cannot show the feature of the instance of the filter is periodically refreshed to enact the updated filtering table. Accordingly, *Massarani* does not anticipate claim 7.

Additionally, as shown above, *Massarani* does not anticipate all the features of claim 1. Since claim 7 depends from claim 1, then all arguments for claim 1 also apply here and *Massarani* does not anticipate all the features of claim 7.

Because claim 14 covers the same subject matter as claim 1, the same distinctions between claim 7 and *Massarani* apply to claim 14. Therefore, the rejection of claims 7 and 14 under 35 U.S.C. § 102(e) has been overcome.

CONCLUSION

In view of the above, Appellants respectfully submit that claims 1, 3-8 and 10-15 are allowable over the cited prior art and that the application is in condition for allowance. Accordingly, Appellants respectfully request the Board of Patent Appeals and Interferences to overturn the rejections and allow the claims.

Hope Shimabuku

Hope Shimabuku
Reg. No. 57,072
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method for filtering incoming data from an external computer network, comprising:

a firewall that is coupled to said external computer network;

a server computer system coupled to an internal computer network;

a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;

receiving, at said firewall, a document from said external computer network;

determining, by said firewall, whether said document is from a known blocked site;

in response to determining that said document is from a known blocked site, blocking, by said firewall, said document without scanning said document;

determining, by said firewall, whether said document is from a known safe site;

in response to determining that said document is from a known safe site, forwarding, by said firewall, said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;

in response to determining that said document is not from a known blocked site or a known safe site, scanning, by said firewall, text fields included in said document for pre-selected keyword(s);

blocking, by said firewall, the document if any of said text fields include content that contains pre-selected keywords;

said server computer system being prohibited from receiving said document in response to said document being blocked; and indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table.

3. The method according to claim 1, wherein the document is allowed to pass per standard service rules if the content does not contain pre-selected keyword(s).

4. The method according to claim 1, further comprising storing an indication in said filtering table of each known safe site that can be passed per standard service rules without having to be scanned for pre-selected keywords.

5. The method according to claim 1, wherein the step of indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of a site to a filtering table further comprises adding the address of the site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords.

6. The method according to claim 1, wherein the addition of a site to the filtering table is implemented using a strong text parsing language.

7. The method according to claim 1, wherein the instance of the filter is periodically refreshed to enact the updated filtering tables.

8. A computer program product in a computer readable medium for use in a data processing system for filtering incoming data from an external computer network, the computer program product comprising:

a firewall that is coupled to said external computer network;

a server computer system coupled to an internal computer network;

a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;

instructions for receiving, at said firewall, a document from said external computer network;

instructions for determining, by said firewall, whether said document is from a known blocked site;

in response to determining that said document is from a known blocked site, instructions for blocking said document without scanning said document;

instructions for determining, by said firewall, whether said document is from a known safe site;

in response to determining that said document is from a known safe site, instructions for forwarding said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;

in response to determining that said document is not from a known blocked site or a known safe site, instructions for scanning, by said firewall, text fields included in said document for pre-selected keyword(s);

instructions for blocking, by said firewall, the document if any of said text fields include content that contains pre-selected keywords;

said server computer system being prohibited from receiving said document in response to said document being blocked; and instructions for indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table.

10. The computer program product according to claim 8, further comprising instructions for allowing the document to pass per standard service rules if the content does not contain pre-selected keyword(s).

11. The computer program product according to claim 8, further comprising instructions for storing an indication in said filtering table of each known safe site that can be passed per standard service rules without having to be scanned for pre-selected keywords.

12. The computer program product according to claim 8, wherein the instructions for indicating that a site that sent said document is a known blocked site by adding, by said firewall, that address of said site to a filtering table further comprises adding the address of said site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords.

13. The computer program product according to claim 8, wherein the instructions for addition of a site to the filtering table are implemented in a strong text parsing language.

14. The computer program product according to claim 8, wherein the instance of the filter is periodically refreshed to enact the updated filtering tables.

15. A system for filtering incoming data from an external computer network, the system comprising:

a firewall that is coupled to said external computer network;

a server computer system coupled to an internal computer network;

a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;

said firewall for receiving a document from said external computer network;

said firewall for determining whether said document is from a known blocked site;

in response to determining that said document is from a known blocked site, said firewall for blocking said document without scanning said document;

said firewall for determining whether said document is from a known safe site;

in response to determining that said document is from a known safe site, said firewall for forwarding said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;

in response to determining that said document is not from a known blocked site or a known safe site, said firewall for scanning text fields included in said document for pre-selected keyword(s);

said firewall for blocking the document if any of said text fields include content that contains pre-selected keywords;

said server computer system being prohibited from receiving said document in response to said document being blocked; and

said firewall for indicating that a site that sent said document is a known blocked site by adding the address of said site to a filtering table.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.